Attorney's Docket No. 047138/257085 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	09/518,583	Confirmation No.: 5843
Applicant(s):	Chee-Seng Chow, et al.	
Filed:	March 3, 2000	
Art Unit:	2134	
Examiner:	Mossadeq Zia	
Title:	SYSTEM AND METHOD FOR ACCESSING A REMOTE SERVER FROM AN INTRANET WITH A SINGLE SIGN-ON	

Docket No.: 047138/257085
Customer No.: 00826

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBSTITUTE APPEAL BRIEF UNDER 37 CFR § 41.37

This Substitute Appeal Brief is filed pursuant to the Notification of Non-Compliant Appeal Brief mailed August 29, 2006, to correct the deficiencies of the Appeal Brief filed on June 5, 2006. Modifications to this Substitute Appeal Brief are limited to an amended Summary of Claimed Subject Matter.

1. ***Real Party in Interest.***

The real party in interest in this appeal is GetThere Inc., the assignee of the above-referenced patent application.

2. ***Related Appeals and Interferences.***

There are no related appeals and/or interferences involving this application or its subject matter.

3. ***Status of Claims.***

The present appeal involves Claims 1-22, which are presently under a final rejection as set forth by the Official Action mailed August 10, 2005. A pre-appeal request was submitted on

November 3, 2005, but the decision of the panel of Examiners found that Claims 1-22 stand rejected because one or more issues are ripe for appeal. The claims at issue are set forth in the attached Claims Appendix.

4. ***Status of Amendments.***

No amendments have been filed subsequent to the final Official Action of August 10, 2005.

5. ***Summary of Claimed Subject Matter.***

The present invention provides a method, system, and computer-readable medium for performing multiple user authentications with a single sign-on. As such, a user may be initially authenticated such as upon accessing a first or local server. This initial authentication also serves to authenticate the user as the user accesses a remote sever. In this regard, a token containing authentication information may be passed to the remote server such that the user can be authenticated by the remote server without entering any additional information. According to the present invention, the token also includes information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. As such, by simply logging on to the first or local server, an account or user profile is created for the user without the user having to also access or enter information at the remote server. The user profile may store information that may be updated and is useful for providing efficient and individualized service to the user.

Independent Claims 1, 21, and 22 recite performing a user authentication, while independent Claim 11 recites a user sign-on interface configured to perform a first user authentication. (Page 3, lines 3-5). FIG. 1 illustrates one embodiment in which an Intranet **102** is connected to a remote server **104**. In one embodiment, the remote server **104** could be a host travel reservation and booking service. (Page 5, lines 23-25). In order to perform a user authentication and gain access to the remote server **104**, the user typically logs onto an Intranet server **120** with a username and password. (FIG. 2A; Page 6, lines 10-17; Page 8, lines 5-10). The user may use the Intranet and resources external to the Intranet once signed onto the Intranet server. (Page 7, lines 1-3).

Independent Claims 1, 21, and 22 also recite selecting a remote server subsequent to said first authentication, while independent Claim 11 recites a link interface configured to select a remote server subsequent to said first user authentication. (Page 3, lines 6-7; Page 5, lines 6-7). Thus, according to one aspect of the present invention, because the Intranet server **120** has already authenticated the user, the user can select a link for the remote server, where the Intranet server **120** sends a token containing authorization information to the remote server **104** causing the remote server to authenticate the user without the user needing to perform a second sign-on. (FIGS. 1 and 2B; Page 7, lines 1-11; Page 8, line 16 – Page 9, line 9).

Furthermore, independent Claims 1, 21, and 22 recite sending a token to the remote server containing authentication information responsive to the first authentication. (Page 3, lines 7-9; Page 5, lines 7-10). Similarly, independent Claim 11 recites a token configured to be sent to the remote server. (Page 3, lines 7-9). In this regard and with reference to FIG. 1, the Intranet server **120** sends an encrypted user identification ("user ID") and time stamp to the remote server **104** (i.e., a token), where the remote server can decode the user ID and time stamp to authenticate the user. (Page 7, lines 11-15). The user is then given access to the remote server **104** and functions available through the remote server. (Page 7, lines 16-17). Figure 6 illustrates the contents of an exemplary authentication token, which takes the form of a credential token **600** in this particular embodiment. The credential token **600** typically includes a username **602**, an expiration time **604**, and a checksum **606**, where the credential token may be encrypted by the Intranet server and placed into a URL for transmission and subsequent user authentication by the remote server. (Page 13, lines 16-21).

Independent Claims 1, 11, 21, and 22 recite that the token also contains information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. With reference to Figure 8, a flowchart is shown which illustrates a method for adding a new user. In step **802**, the user performs an Intranet user authentication process. (Page 16, line 12). In decision step **804**, the Intranet server determines whether the user is a new user. (Page 16, lines 12-14). If so, the Intranet server sets a new user flag in step **806**. (Page 16, lines 14-15). In step **808** the Intranet server forms the fields for the token, including the new user flag. (Page 16, lines 19-20).

In addition to or instead of providing information regarding a new user, independent Claims 1, 11, 21, and 22 recite that the token can include information regarding a change or update to an existing account. Referring to Figure 9, for example, a flowchart for a method for updating a user's profile is shown. User profile information may be stored at the remote server. (Page 18, line 7). The user profile information may include information about the user that may help the remote server provide efficient service to the user. (Page 18, lines 8-9). For instance, if the remote server is a travel reservation and booking service, user profile information may include dietary choices, seating preferences, travel spending limits, and other information specific to a given user. (Page 18, lines 9-13). In step **902** of FIG. 9, the user performs an Intranet user authentication. (Page 18, line 18). In decision step **904**, the Intranet server determines if the user wishes to create a new user profile or update an existing user profile. (Page 18, lines 18-20). If so, the Intranet server places the user profile data into strings in step **906**. (Page 18, lines 21-23). In step **908**, the Intranet server forms the fields for the token, including the user profile data. (Page 18, lines 24-26).

Independent Claims 1, 21, and 22 recite decoding the authentication information, wherein decoding the authentication information induces a second user authentication, while independent Claim 11 recites a decoder configured to decode the authentication information and induce a second user authentication. (Page 3, lines 9-12; Page 5, lines 10-13). As indicated above, the Intranet server **120** sends a token containing authorization information to the remote server **104** causing the remote server to authenticate the user without the user needing to perform a second sign-on. (FIGS. 1 and 2B; Page 7, lines 1-11; Page 8, line 16 – Page 9, line 9). In this regard, when the user attempts to access the remote server and the services offered thereby, the token including the information regarding the user profile is transmitted to the remote server. (FIG. 9; Page 19, lines 15-17). The remote server then receives and decrypts the token in step **922** and, if the remote server determines the token is valid, the token is examined for user profile information in step **928**. If user profile information is found, and if the remote server software is set to enable updating user profile information, then in step **938**, the remote server creates a new user profile or updates any existing user profile. (Page 19, line 23 – page 20, line 1). More specifically and as shown in Figure 3, Intranet server code **302** may include remote server

module **304** and an encryption module **306**. (Page 9, lines 19-20). When activated, the remote server module **304** may examine the status of the user's authentication access to the Intranet, and if authenticated, the remote server module **304** may respond to a remote link request **312** by providing a URL with an encrypted token **314** to the user's browser for use in accessing remote server code **320**. (Page 9, lines 25 – Page 10, line 5). Once the URL with the encrypted token **314** has been provided, the user's browser **308** may transmit the URL with the encrypted token to the remote server code **320** along URL data path **316** that extends to the remote server. (Page 10, lines 23-26). In one embodiment, the CGI module **322** of the remote server receives the URL and decodes the URL and decrypts the token. (Page 11, lines 1-4). The CGI module may then pass the decrypted token to remote server application **324** for authentication of the user. (Page 11, lines 4-7).

Independent Claim 21 includes means-plus-function language. In particular, Claim 21 generally recites means for performing a first user authentication and means for selecting a remote server. The means for performing a first user authentication generally includes a workstation running a browser program that a user accesses through a computer interface having associated software and/or hardware to perform a first user authentication. (See Page 7, lines 1-26; Page 9, lines 10-18). The means for selecting a remote server also comprises a workstation operating a browser program from which a user selects a remote server, for example, by clicking a link from a list of links presented on the user's browser. (See Page 7, lines 1-5; Page 9, lines 3-9). Claim 21 also recites means for sending a token to the remote server. The means for sending the token is comprised of a network such as the internet, wide area network, local area network, or other computer interface. (See Figure 1; Page 5, line 22 – Page 6, line 2; Page 10, lines 23-26). In addition, Claim 21 recites means for decoding the authentication information. The decoding could be performed by transmitting a universal resource locator (URL) with an encrypted token to remote server code along a transmitted URL data path. (See Figure 3; Page 10, lines 23-26). As such, the means for decoding the authentication information comprises a remote server operating to decode the authentication information. In one exemplary embodiment, the remote server code could include a CGI module, a remote server application, and an error handler, where the CGI module may decode the URL and decrypt the decrypted

token. (See Page 10, line 26 – Page 11, line 7). In alternative embodiments, the remote server code may include alternative interface code architectures for the CGI module. (See Page 11, lines 8-10).

Furthermore dependent Claims 5 and 15 recite that the information regarding an account for the user in the token includes a new user flag. As indicated above and with reference to FIG. 8, the Intranet server determines whether the user is a new user. (Page 16, lines 12-14). If so, the Intranet server sets a new user flag and forms the fields for the token including the new user flag. (Page 16, lines 14-15 and 19-20).

Dependent Claims 6 and 16 recite that the remote server creates a new user account in response to the new user flag. In this regard, upon the first attempt of the user to access the remote server and the services offered thereby, the token including the new user flag is transmitted to the remote server. (Page 17, lines 4-5). The remote server then receives and decrypts the token in step **822** and, if the remote server determines the token is valid, the new user flag status is tested in step **828**. (Page 17, lines 6 and 11-12). If the new user flag is set and if the remote server software is set to enable adding new users, then in step **834**, the remote server tests to see if the username is already in use. (Page 17, lines 24-26). If not, then, in step **838**, a new user account is established, and, in step **840**, the user is authenticated. (Page 18, lines 1-4).

As such, the method, system, and computer-readable medium of the present application allow a user to access a remote server utilizing a single sign-on authentication. The present invention eliminates the need for additional sign-on authentication for the user when a user accesses a first server, such as an Intranet server, and wishes to also access remote servers. Thus, the method, system, and computer-readable medium prevent the user from having to remember and enter additional sign-on information, such as a different password, for each remote server, which provides increased security for the user's authentication information.

6. ***Grounds of Rejection to be Reviewed on Appeal.***

(i) Claims 1-4, 7-14, and 17-22 stand rejected under 35 U.S.C. § 102(e), as being anticipated by U.S. Patent No. 6,453,353 to Win et al.; and

(ii) Claims 5, 6, 15, and 16 stand rejected under 35 U.S.C. § 103(a), as being unpatentable over Win in view of U.S. Patent No. 6,144,959 to Anderson et al.

7. ***Argument.***

(i) Independent Claims 1, 11, 21, and 22

Win discloses that a single sign-on may be utilized to give a user access to authorized web resources, where access to web resources is based on the user's role in the organization. Thus, users are not required to log in individually to each web resource. More specifically, the user accesses an Access Server that stores a log-in page, Authentication Client Module, and Access Menu Module. The Authentication Client Module verifies a user's name and password with a Registry Server, where the Registry Server stores information about users (*e.g.*, name, password, and locale information), resources (e.g., web pages, web sites, etc.), and roles (*e.g.*, employee, customer, distributor, etc.) of the users. If the name and password are correct, the Authentication Client Module reads the user's roles from the Registry Server, and then encrypts and sends this information in a cookie to the user's browser. After selecting a resource, the browser sends an open URL request and cookie(s) to a Protected Web Server, which is protected by a Runtime Module. The Runtime Module decrypts information contained in the cookie and uses the information to verify that the user is authorized to access the resource. The resource uses the cookie to return information that is customized based on the user's name and roles.

In contrast to the disclosure of Win described above, independent Claims 1, 11, 21 and 22 recite a method, systems, and a machine-readable medium for performing multiple user authentications with a single sign-on by performing a first user authentication, selecting a remote server, and sending a token to the remote server that contains authentication information responsive to the first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. The authentication information is then decoded to induce a second user authentication.

User profile information may be stored by the remote server. (Page 18, line 7). The information regarding a new or updated user account that is included in the token of the claimed invention may come in various forms. With respect to the embodiment of Figure 8 of the present

application, the token may include fields, including a field for a new user flag that is set when the Intranet server detects a new user. (Page 16, lines 12-15). The embodiment depicted by Figure 9 of the present application adds the capability to transmit new or updated user profile information to the remote server. The remote server may store user profile information that may help the remote server, such as a travel reservation and book service, and provide efficient service to the user (*e.g.*, dietary choices, seating preferences, travel spending limits, *etc.*). Once the token is determined to be valid, the token is examined for user profile information, and the remote server may create an account for a new user or update an account for an existing user depending upon the user profile information. Thus, the multiple user authentication of the claimed invention not only provides a single sign-on procedure, but also provides a capacity for efficiently creating or updating user accounts at the remote server.

In the Response to Arguments, the Official Action finds that "Win teaches sending the cookies with the updated information to remote servers." In addition, the Official Action alleges that information regarding user configuration or user roles may be modified or updated. The Official Action interprets Win as disclosing that user information corresponds to "roles," while "role cookies" are sent to remote resources. Moreover, the Official Action finds that Win discloses that new account information can be sent to remote resource with the role cookie to be updated by a user or an administrator.

While Win discloses a single sign-on through an Access Server to access protected web resources, Win does not disclose sending a token to a remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user, as recited by independent Claims 1, 11, 21 and 22. Win arguably discloses that the URL request and associated cookies contain authentication information, as the cookies contain profile information and a list of the user's roles. The profile information, such as username and password, allows the user to log in to the system and is used to verify that the user is authorized to access a resource, while the roles, such as employee or supplier, define the resources that are available to the user.

However, updating the profile information of Win may be achieved when the user updates profile or locale information within the Profile Management Service of Authentication Client module (see col. 9, line 33-35), which is associated with the Access Server (see Figure 4 of Win), not the remote resources, such as the remote server that maintains the current user account information pursuant to the claimed invention. Moreover, Win discloses that an administrator may find, list, create, delete, and modify user role records (see col. 13, lines 8-10) using an Administration Application that is executed or supervised by a Protected Server coupled to a Registry Server (see col. 6, lines 27-31). Therefore, updated information is not included with the cookies since updating occurs at the Access Server or Registry Server (see Figures 1 and 4 of Win). Similarly, Win does not disclose that the cookies contain information regarding a new account for the user. Simply providing the capability to update or add a new account is significantly different than providing information regarding a new account or an update to an existing account with a token to a remote server, as recited by the claimed invention.

The Examiner relies upon col. 8, line 46 – col. 9, line 40 of Win for the proposition that user information relates to "roles" and that "role cookies" are sent to remote resources. Assuming that the Examiner's characterization of Win is correct, the specific portion of Win relied upon only discloses that users may change their account profiles at the Access Server. This is unlike the claims of the present application, as described above, in which tokens reflective of new or updated user account information are sent to a remote server. In this regard, Win nowhere discloses that the cookies contain information regarding an update to an existing account or information regarding a new account in addition to containing authentication information.

The Examiner further relies upon col. 7, lines 58-67 of Win as disclosing that cookies may be sent with updated information. However, this particular portion of Win pertains to "configuration changes." Win discloses that an example of a configuration change could be adding resources to the Protected Server, where Win describes examples of resources as web pages, web sites, a web-enabled database, and an applet (see col. 5, lines 14-20). Thus, the configuration changes disclosed by Win correspond to system level changes rather than information regarding an account for a user. In particular, configuration changes are distinctly

different than information regarding an update to an existing user's account or information regarding a new account for a user, as recited by the claimed invention. As such, the Examiner mischaracterizes configuration changes as corresponding to "user configurations," as stated in the Response to Arguments.

Also, in the Response to Arguments the Official Action finds that "Win teaches that new account information can be sent to a remote resource (or server) with the 'role cookie' which can be updated by either the Administrator or a user." However, the Official Action again relies upon the portion of Win that discloses configuration changes (col. 7, line 52 – col. 8, line 23), which as described above, is distinctly different from tokens containing information regarding an update to an existing account or information regarding a new account for the user, as recited by the claimed invention. Not only do the cited portions of Win not teach or suggest the claimed invention, but no other portions of Win disclose independent Claims 1, 11, 21, and 22.

Nor does the remaining cited reference, U.S. Patent No. 6,144,959 to Anderson et al., taken alone or in combination with Win, teach or suggest sending a token to a remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user, as recited by independent Claims 1, 11, 21, and 22. Anderson discloses a system and method for managing user accounts in a communication network. The system is capable of using a single set of credentials to access servers that are centrally located and managed such that an administrator does not have to maintain separate accounts on a shared workstation for all users. A user logging in at a client workstation provides credentials through a log-in interface. An authentication process is employed to authenticate the user to the local client, as well as to one or more servers. The authentication process compares credentials contained in a request for access generated by the client to entries within a domain database. If the credentials match, the domain authentication process allows access to the server process and resources. Moreover, Anderson discloses that there may be a client that provides an administrator access to a directory services database contained within a server. For example, the directory services database may support a client workstation object, where the client workstation object may include log-in information. The log-in information could include a dynamic log-in

flag that is used to indicate whether user information should be retrieved from the client workstation object to create a user account on a client. Thus, when the log-in process is initiated at the client and inspects the workstation object, the log-in process may need to identify if a user account should be created in the local access database of the client.

Although Anderson arguably discloses sending authentication information in the form of credential information, the credential information does not include information regarding a new account and/or an update to an existing account for a user, as recited by the claimed invention. Anderson discloses that credential information corresponds to username, password, log-in information for a database, a log-in script, retinal scan, or fingerprint information (col. 2, lines 4-18). Thus, the credential information is only used for authentication rather than for authentication and updating an existing user account and/or adding a new user account, as recited by the claimed invention. In particular, Anderson discloses that credential information is transmitted from the client to the directory services database for authentication and allowing the user access to the server process and any server resource associated with the user account (col. 9, lines 48-56). Therefore, Anderson does not disclose that information regarding a new account and/or an update to an existing account is included with the credential information.

In addition, even though Anderson discloses a dynamic login process that can determine whether login information maintained at a remote server contains a login flag for determining whether a user account should be created in the local access database, the login information and flag are not contained within a token that is sent to a remote server as in the claimed invention as the login information and dynamic login flag are already located in the directory services database that is associated with a remote server (see Figures 3A and 3B). Thus, the login information and dynamic login flag are not contained within a token that is sent to the remote server, as each is located at the remote server and is simply accessed during the dynamic login process at the client. In contrast, Anderson discloses that workstation configuration information is transferred from the server to the client where the authentication process determines whether the user account exists in the local access database (col. 16, lines 26-42). If a user account does not exist, the authentication process creates a user account in the local access database (col. 17, lines 2-5). Therefore, even if Anderson discloses sending information regarding a new account,

the information is sent from the server to the client, while the authentication information for providing the user access to the server resources is provided from the client to the server, which is unlike the claimed invention in which both are included in a token.

Thus, neither Win nor Anderson, taken individually or in combination teach or suggest including information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user in a token that is sent to a remote server, as recited by independent Claims 1, 11, 21, and 22. Thus, the rejection under 35 U.S.C. § 102(e) is overcome. Since the independent claims are patentably distinct from the cited references, the claims that depend therefrom are also distinguishable from the cited references for at least the same reasons since the dependent claims include each of the elements of a respective independent claim.

(ii) Dependent Claims 5, 6, 15, and 16

Applicants submit that each of the dependent claims are distinguishable from the cited references for at least those reasons discussed above with respect to independent Claims 1, 11, 21, and 22. Applicants also submit that a number of dependent claims, including Claims 5, 6, 15, and 16, are further distinguishable from the cited references, including Anderson. The Examiner acknowledges that Win does not teach dependent Claims 5, 6, 15, and 16, but instead relies upon Anderson to overcome Win's shortcomings. In this regard, Claims 5 and 15 recite that the information regarding an account for the user in the token includes a new user flag, while Claims 6 and 16 recite that the remote server creates a new user account in response to the new user flag.

As described above, although Anderson discloses that a dynamic log-in flag 317 may be utilized, the flag is maintained in a directory services database 223 that is associated with a server 103A, which is transmitted to the client 102A during the log-in process (see Figures 2A and 3A of Anderson). The log-in process 207 inspects the client workstation object 305G to determine whether a new user account should be created in the local access database 203 maintained in the client (col. 13, lines 48-55). In this regard, the dynamic log-in flag is not contained within a token that is sent from the client to the server, as recited by Claims 5, 6, 15,

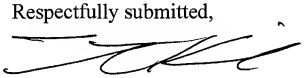
and 16, as the client workstation object, including the dynamic login flag, is sent from the server to the client to determine whether a new user account should be set up at the client. Therefore, the dynamic user flag is not contained within a token that includes authentication information and information regarding a new account and/or an update to an existing user account, as recited by the claimed invention.

Thus, neither Win nor Anderson, taken individually or in combination, teach or suggest that the information regarding an account for the user in the token includes a new user flag, as recited by dependent Claims 5 and 15, or that the remote server creates a new user account in response to the new user flag, as recited by dependent Claims 6 and 16. Consequently, Applicants submit that, for at least those reasons above, the rejection of dependent Claims 5, 6, 15, and 16 under 35 U.S.C. § 103(a) is overcome.

CONCLUSION

For the above reasons, it is submitted that the rejections of Claims 1-22 are erroneous and reversal of the rejections is respectfully requested. A Claims Appendix containing a copy of claims involved in the appeal, an Evidence Appendix, and a Related Proceedings Appendix are attached.

Respectfully submitted,



Trent A. Kirk
Registration No. 54,223

CUSTOMER NO. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

ELECTRONICALLY FILED USING THE EFS-WEB ELECTRONIC FILING SYSTEM OF THE UNITED STATES PATENT & TRADEMARK OFFICE ON October 6, 2006.

Claims Appendix

1. (Previously Presented) A method of performing multiple user authentications with a single sign-on, comprising:

performing a first user authentication;

selecting a remote server subsequent to said first authentication;

sending a token to said remote server containing authentication information responsive to said first authentication, wherein the token also contains information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user; and

decoding said authentication information, wherein said decoding said authentication information induces a second user authentication.

2. (Original) The method of claim 1, wherein said sending includes sending said token within a universal resource locator.

3. (Original) The method of claim 2, wherein said token includes a timestamp.

4. (Original) The method of claim 2, wherein said token is encrypted.

5. (Previously Presented) The method of claim 1, wherein the information regarding an account for the user in said token includes a new user flag.

6. (Original) The method of claim 5, wherein said remote server creates a new user account in response to said new user flag.

7. (Previously Presented) The method of claim 1, wherein the information regarding an account for the user in said token includes user profile update information.

8. (Original) The method of claim 7, wherein said remote server updates a user profile in response to said user profile update information.

9. (Original) The method of claim 1, wherein said first user authentication occurs within an Intranet.

10. (Original) The method of claim 1, wherein said second user authentication occurs within said remote server.

11. (Previously Presented) A system for performing multiple user authentications with a single sign-on, comprising:

a user sign-on interface, configured to perform a first user authentication;

a link interface, configured to select a remote server subsequent to said first user authentication;

a token configured to be sent to said remote server, said token containing authentication information responsive to said first user authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user; and

a decoder configured to decode said authentication information, said decoder further configured to induce a second user authentication.

12. (Original) The system of claim 11, wherein said token is coupled to a uniform resource locator.

13. (Original) The system of claim 12, wherein said token includes a timestamp.

14. (Original) The system of claim 12, wherein said token is encrypted.

15. (Previously Presented) The system of claim 11, wherein the information regarding an account for the user in said token includes a new user flag.

16. (Original) The system of claim 15, wherein said remote server creates a new user account in response to said new user flag.

17. (Previously Presented) The system of claim 11, wherein the information regarding an account for the user in said token includes user profile update information.

18. (Original) The system of claim 17, wherein said remote server updates a user profile in response to said user profile update information.

19. (Original) The system of claim 11, wherein said first user authentication occurs within an Intranet.

20. (Original) The system of claim 11, wherein said second user authentication occurs within said remote server.

21. (Previously Presented) A system for performing multiple user authentications with a single sign-on, comprising:

means for performing a first user authentication;

means for selecting a remote server subsequent to said first authentication;

means for sending a token to said remote server containing authentication information responsive to said first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user; and

means for decoding said authentication information, wherein said means for decoding said authentication information induces a second user authentication.

22. (Previously Presented) A machine-readable medium having stored thereon instructions for performing multiple user authentications with a single sign-on, which, when executed by a set of processors, cause said set of processors to perform the following:

performing a first user authentication;

selecting a remote server subsequent to said first authentication;

sending a token to said remote server containing authentication information responsive to said first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user; and

decoding said authentication information, wherein said decoding said authentication information induces a second user authentication.

Evidence Appendix

No additional evidence is provided.

Related Proceedings Appendix

There are no related proceedings.